Michael Balboni

President and Managing Director of RedLand Strategies

Friday, November 22, 2019, 11 AM

250 Broadway, Senate Hearing Room - 19th Floor, New York, NY 10007

Companies should be required to handle data in a way that not only ensures privacy, but also security. These two concepts cannot be separated.

Continuous monitoring of your data and breach notification if your data is compromised. Ready access to your data in data centers that are highly available, resilient and secure.
You own your data and it should not be processed for advertising purposes.

Companies that have consumer data should comply with all State and international privacy and security standards. This compliance should be certified and audited. Companies should provide a "transparency report" so that users can view the transactions involving their data. Companies should be ever vigilant to ensure the integrity of the data from "governmental backdoors".

But in protecting the data, it is important to carve out the above protections if the personal data is used to ensure data. For instance, many security platforms will monitor data through its addresses and the way it behaves. If a data packet is coming for an unknown source, some security providers either compare the address and configuration to a known data base of good ware and malware. But sometimes, this comparison is not good enough and the security strategy is to place the unknown item in and artificial environment and have the program execute and determine if the item is malicious or benign. This is called "sandboxing".

Sandboxing data should not be placed in the same bucket of concern as the selling of personal data for advertising.

The GDPR is seen as the first comprehensive step towards securing someone's privacy in cyber space. But the law had significant flaws such as requiring that companies take "reasonable steps" to ensure the safety of the data. This is too vague and new regulations should require compliance with security standards that have proven to be effective such as the National Institute of Standards and Technology, (NIST). The NIST framework provides a checklist of steps necessary to bring companies to a better state of security and begins to provide a level of uniformity for cyber security.

In addition, other exemptions should apply. The regulations should be written to ensure that access to data should be preserved for security purposes and if the owner permits the access. Also, drafters of the legislation should be mindful of legal retention requirements before granting a broad "right of erasure" of the data.

Measures that would harm the free use and transmittal of data should be discouraged. One such item would be the creation of a broad private rights of action. The problem is that to date, courts have been reluctant to certify a class action for individuals who's date is compromised and exposed. The challenge is causation. Does a data breach necessarily result in harm to every person so exposed? This is an area of the law that is still developing.

Another very important area is identity management. Who is allowed into the digital operating environment? Identity and Access Management verifies how enterprises allow their employees to access critical data and applications by defining and managing privileges provided to account holders. The threat of insider threats, employee negligence and spoofed credentials can be mitigated by effective Identity and Access Management. The good news is that the ease of use are getting better. Much has been made of multifactor authentication. With the universality of the I phone, we now have a way to determine that you are you. The phone is registered to you. You can utilize an anachronistic but still valuable password/login, and more and more phones have a biometric feature, thumbprint. These three things go along way in ensuring that you are you. Combined with the right protocols and access privileges, it is much easier to know who is in your environment.

Privacy begins with the individual's access to safe and secure data. If your data is stolen or compromised. Otherwise, the "right to be forgotten" will simply not exist.

Must-Have

- Technology neutral security requirements
- Security as legitimate use of personal data/security as legal basis exempt from consent
- Ability to transfer data across border
- Exceptions to right of access (security, other people privacy)
- Exceptions to right to erasure (legal compliance; security; only data provided by data subject)

Must-Not-Have

- Consent as the sole basis for processing
- Data localization/data sovereignty
- Onsite audit rights for customers/controllers/regulators
- Broad private right of action
- Set breach notification timing (in days or hours)
- Absolute or overly generic right of access or right to erasure

Nice-To-Have

- Less stringent requirements for business contact information
- Employee data carveout
- Can-Live-With
- Cross border data transfer requirements

- Data protection impact assessments
- Privacy and Security by Design
- Security controls (as long as they are tech neutral)
- Vendor contracts / data processing agreements
- Records of processing
- Prior consultation for high risk processing